Prévention et répression de la criminalité sur Internet

Gérard, Philippe; Willems, Valerie

Published in:
Internet face au droit

Publication date:
1997

Document Version
le PDF de l'éditeur

Chapitre 5 - Prévention et répression de la criminalité sur Internet

par Philippe GERARD* et Valérie WILLEMS+

* Avocat au Barreau de Bruxelles, attaché de recherches au C.R.I.D
+ Consultant, Cullen International.

I. Introduction

On pouvait lire dans une édition récente du quotidien français « Le Monde » :

« Internet favorise la pédophilie. Les pédophiles peuvent faire du racolage sur les forums de discussion, s'échanger des adresses et des images ».	*« Internet permet d'arrêter les pédophiles. En 1995, au Royaume-Uni, avec l'opération « starbust », la police a démantelé un réseau de pornographie enfantine ».*
« Internet facilite l'espionnage industriel. Des robots de recherche traquent tous les documents émis par un concurrent. Les entreprises s'intoxiquent mutuellement ».	*« Grâce à Internet, les entreprises peuvent s'informer et améliorer ainsi leurs activités et leur productivité ».*
« Les fanas d'Internet s'intéressent surtout aux messageries roses et aux sites érotiques. Certains fournisseurs d'accès français ayant une clientèle de particuliers estiment que l'accès aux services et aux forums érotiques représentent près de la moitié de leur trafic (Rapport de l'A.F.T.E.L.) ».	*« Le sexe fait partie des « usages » auquel une part importante des consommateurs se familiarisent avec les technologies et les services nouveaux. Cette situation ne fait que confirmer ce que l'on a pu constater au démarrage du magnétoscope, de la télévision payante ou, bien sûr du Minitel.* (Rapport de l'A.F.T.E.L.) »
« Internet facilite les trafics en tous genres : médicaments, drogues, armes, etc. »	*« Internet permet une meilleure diffusion de l'information médicale ».*
« Internet favorise la communication entre terroristes. L'autorisation de cryptage, qui tend à se généraliser sous la pression des entreprises commerciales, ne fera qu'accentuer ce phénomène ».	*« Internet peut aider à repérer des terroristes, en fonction des machines d'où ils émettent leurs messages. S'ils sont cryptés, ils pourront être déchiffrés sur demande des autorités policières et judiciaires, car les législations tendent actuellement à imposer le principe du tiers de confiance. »*

Ces quelques extraits tirés du Monde des 17 et 18 novembre 1996[360], doivent nous aider à démystifier le phénomène d'Internet. Internet n'est ni mal ni bien. Il est sans doute bon de le répéter. Il ne s'agit ni plus ni moins

360 Page 33.

que d'un moyen de communication. Le téléphone, la télévision sont-ils « bons » ou « mauvais » ? Le lecteur ne nous en voudra pas, on l'espère, de limiter notre exposé à des considérations plus juridiques.

En principe, les auteurs d'infractions peuvent abuser de façons très diverses des réseaux informatiques comme Internet ou des réseaux de services connectés en lignes, pour parvenir à leurs fins. Le large éventail des infractions implique toutefois que l'on opère une distinction grossière entre deux catégories principales d'infraction.

D'une part, il y a des infractions spécifiquement dirigées contre les réseaux et les systèmes de traitement de données qui y sont connectés. D'autre part, il est des infractions pour lesquelles des réseaux, tel qu'Internet, servent de support de communication.

II. Les délits informatiques

Le recours à Internet permet, comme dans le cas d'autres réseaux, de commettre des infractions portant spécifiquement atteinte à l'informatique, et ce peut-être même davantage, puisque Internet implique l'utilisation de modems dans un environnement ouvert. Si les premiers cas de délinquance informatique ont été révélés par la presse pendant les années soixante, cette forme de délinquance s'attaque aujourd'hui à la plupart des intérêts, qu'il s'agisse de l'intérêt public, économique, socioculturel, ou qu'il s'agisse d'intérêts d'ordre purement privé.

Les rapports élaborés notamment au sein d'organisations internationales[361] ont certainement contribué à rendre conscients les législateurs nationaux de l'importance d'adopter des réglementations spécifiques répondant, selon les termes du Conseil de l'Europe, aux « nouveaux défis de la criminalité informatique »[362]. Que recouvre cependant ce phénomène de criminalité informatique ?

II.1. Notions

Le caractère polymorphe de cette forme de criminalité explique qu'aucune organisation internationale, à ce jour, n'ait consacré une définition précise de celle-ci.

La criminalité informatique recouvre en effet des phénomènes aussi variés que l'accès non autorisé à un système informatique, l'interception de communications électroniques, la reproduction illicite de programmes d'ordinateur ou de données informatiques, les manipulations de données en tous genres, qu'il s'agissent de manipulations sur les salaires, polices d'assurance ou autres opérations bancaires.

Une définition émanant d'un groupe d'experts de l'O. C. D. E. peut toutefois être relevée bien qu'elle n'ait pas été reprise, étant donné sa formulation large, dans le rapport élaboré par l'organisation internationale en 1986[363].

361 OCDE, "La fraude liée à l'informatique : analyse des politiques juridiques, Paris, 1986, Conseil de l'Europe, "Rapport final du Comité européen pour les problèmes criminels", Strasbourg, 1990, Nations Unies, Huitième Congrès pour la prévention du crime et le traitement des délinquants, Rapport, New York, 1991; Voir aussi Chambre de Commerce Internationale, Rapport adopté par le Comité Directeur, "Délinquance associée à l'informatique et droit pénal : le point de vue de la communauté économique internationale", Paris, 1988, Document n° 373/76 Rev.

362 Recommandation n° (89) 9 du Comité des Ministres du Conseil de l'Europe sur la criminalité en relation avec l'ordinateur.

363 OCDE, "La fraude liée à l'informatique : analyse des politiques juridiques", *op. cit.*

L'abus informatique y est entendu comme *« tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou une transmission de données »*.

Dans un souci plus pragmatique, l'O. C. D. E. , puis le Conseil de l'Europe, ont préféré recourir à une énumération d'aetes répréhensibles, pour lesquels une initiative législative est recommandée.

Le Conseil de l'Europe a ainsi élaboré deux listes, la première dite « minimale » décrit les infractions pour lesquelles une politique devrait être mise en place alors que la deuxième, facultative, regroupe des infractions pour lesquelles un consensus n'a pu être dégagé au sein du Conseil de l'Europe quant à leur incrimination pénale[364].

La liste minimale comprend les infractions de fraude informatique, de faux en informatique, de dommages affectant des données ou des programmes informatiques, de sabotage informatique, d'accès non autorisé à un système informatique ou à un réseau, d'interception non autorisée d'un programme informatique protégé, de reproduction non autorisée d'un programme informatique protégé et de reproduction non autorisée d'une topographie.

La liste optionnelle regroupe les infractions d'altération de données ou de programmes informatiques, d'espionnage informatique, d'utilisation non autorisée d'un ordinateur et d'utilisation non autorisée d'un programme informatique protégé.

On notera encore que, sur le plan de la procédure, le Conseil de l'Europe a adopté en 1995 une Recommandation sur les « Problèmes de procédure pénale liés à la technologie de l'information »[365]. Celle-ci contient en son annexe plusieurs principes que le Comité des Ministres recommande aux Etats de suivre dans leurs réformes législatives. Ces principes concernent notamment les perquisitions, la surveillance des réseaux, la coopération internationale ou encore la preuve électronique.

Plus récemment, on notera encore, au plan international, les recommandations formulées par l'Association Internationale de Droit Pénal sur les « infractions informatiques et autres crimes contre la technologie informatique »[366]. Ces recommandations, fruit d'une réflexion partagée à Rio de Janeiro, en 1994, prônent outre l'adoption de mesures préventives, l'incrimination d'abus tels le trafic des mots de passe ou la distribution de virus, par exemple.

364 Ces listes se trouvent en annexe du rapport du Comité européen pour les problèmes criminels du Conseil de l'Europe sur la criminalité en relation avec l'ordinateur, *op. cit.*

365 Recommandation R (95) 13 intitulée « Problèmes de procédure pénale liés à la technologie de l'information », adoptée par le Comité des Ministres du Conseil de l'Europe le 11 septembre 1995.

366 Revue Internationale de Droit Pénal, Vol. 66, p. 27.

II.2. Situation en Belgique

Face à ces phénomènes divers, de nombreux états, notamment européens ont adopté des législations spécifiques à cette forme de criminalité.

Nous ne disposons toutefois pas, en Belgique, d'initiative législative générale en matière de « criminalité informatique » comparable à la « Wet computer criminaliteit »[367] des Pays-Bas, la loi « Godfrin » française[368] ou encore le « Computer Misuse Act » britannique de 1990.

De manière générale, la répression des infractions informatiques a donc été poursuivie, jusqu'à présent, sur la base des dispositions existantes du Code pénal belge.

II.2.1. Le droit pénal traditionnel

Avant d'examiner quelques cas d'application du Code pénal à la répression de la criminalité informatique, il convient de rappeler certains principes de base de droit pénal qui limitent dans une certaine mesure, son application à ces formes de criminalité.

II.2.2. Le Code pénal et ses principes d'interprétation

En vertu de la Constitution, nul ne peut être poursuivi que dans les cas prévus par la loi et dans les formes qu'elle prescrit (article 12). Par ailleurs, son article 14 prévoit que nulle peine ne peut être établie et appliquée qu'en vertu d'une loi. Ce dernier principe a pour corollaire que la loi pénale est d'interprétation stricte et que son application par analogie est interdite.

En d'autres mots, pour appliquer une disposition pénale à des faits que le législateur était dans l'impossibilité absolue de prévoir à l'époque de l'adoption d'une loi, ce qui, à propos de l'informatique est un euphémisme fréquent vu l'âge respectable de la grande majorité des dispositions du Code Pénal, une double condition doit être remplie : la volonté du législateur d'ériger des faits de cette nature en infraction doit être certaine; les faits doivent pouvoir être compris dans la définition légale de l'infraction[369].

Dans ces limites, une interprétation évolutive du Code pénal est donc permise. En guise d'illustration, on rappellera que la Cour de Cassation, en 1990[370], a confirmé l'application de l'article 383 du Code Pénal à

367 Loi du 13 mars 1993.

368 Loi n°88-19 du 5 janvier 1988 et loi n°92-685 du 22 juillet 1992

369 Cass , 25 janvier 1956, *Pas.*, 1956, I, p. 534; Cass., 21 janvier 1957, *Pas.*, 1957, I, p 583; Cass., 4 mai 1988, *R D.P.*, 1988, p. 958

370 Cass., 11 septembre 1990, *Pas* , 1991, I, p 37.

l'exposition, la vente et la distribution de cassettes vidéo pornographiques, alors que le texte original de cet article réprime l'exposition, la vente et la distribution de figures ou d'images contraires aux bonnes moeurs.

II.2.3. Application du Code pénal aux infractions les plus fréquentes

Dans le domaine informatique, les faits en cause sont souvent la reproduction illicite de programmes d'ordinateur et la vente des copies réalisées, la manipulation de données informatiques ou, encore, l'accès illicite à un système informatique. Les dispositions pénales les plus invoquées sont celles sanctionnant le vol, l'abus de confiance ou encore le faux en écriture, ce qui peut mener à des interprétations quelque peu "spectaculaires" des juridictions saisies.

Ainsi, en est-il dans la célèbre affaire Bistel mettant en cause, à la fin des années 80, deux personnes qui avaient réussi à accéder de manière illicite au système Bistel du gouvernement belge permettant la consultation de bases de données et la messagerie électronique. Elles y avaient pénétré en utilisant les codes et mots de passe obtenus à l'époque du service militaire d'un des deux prévenus, effectué au sein du cabinet du Premier Ministre.

C'est au prix d'efforts louables de raisonnement que la Cour d'Appel de Bruxelles, en 1991[371], considéra que cet accès illicite constituait en réalité l'interception indue d'une communication, réprimée à l'époque par la loi de 1930 sur la télégraphie et la téléphonie avec fil, en constatant que, étant donné que Bistel était relié au système public de télécommunications, les données stockées dans le système Bistel étaient des « communications confiées à la Régie ». L'accès illicite à celles-ci constituaient dès lors une interception illégale de la communication.

S'agissant des principaux arguments invoqués par les victimes, deux qualifications pénales - le vol et le faux en écriture - vont retenir notre attention.

II.2.4. Le vol de programmes ou de données informatiques ?

Indépendamment de la protection éventuelle par le droit d'auteur des programmes d'ordinateur originaux, l'assimilation de la copie illicite de programmes ou données informatiques à l'infraction de vol au sens de l'article 461 du Code pénal[372] soulève toujours bien des interrogations. Cette disposition requiert la réunion de trois éléments constitutifs : une chose, une soustraction et une intention frauduleuse. Les questions sont

371 Bruxelles, 24 juin 1991, *R D P.*, 1991, p. 340.

372 Article 461 paragraphe 1 du Code pénal : "Quiconque a soustrait frauduleusement une chose qui ne lui appartient pas, est coupable de vol".

dès lors les suivantes : une donnée informatique, un programme d'ordinateur peuvent-ils être considérés comme des choses susceptibles d'être soustraites ? La copie non autorisée équivaut-elle à une soustraction ?

Examinons ces questions à la lumière de la jurisprudence, de la doctrine et des conditions établies par la Cour de Cassation pour qu'il puisse y avoir interprétation extensive des dispositions du Code pénal.

II.2.5. La volonté du législateur d'ériger ces faits en infraction est-elle certaine ?

Une partie de la doctrine soutient qu'il n'y a pas volonté du législateur de considérer la copie non autorisée de programmes d'ordinateur ou de données informatiques comme un vol. En effet, "le législateur a introduit un système de protection et de sanctions (y compris pénales) spécifiques aux droits de propriété intellectuelle; la protection offerte à l'information par des dispositions particulières (celles du droit d'auteur, du droit des brevets, celles concernant le secret) indique clairement que la volonté du législateur est que la protection de l'information reste exceptionnelle et spécifique à certaines catégories précises et ne soit pas considérée comme globale..."[373]. A l'inverse, une autre partie de la doctrine considère que les différents systèmes de protection ne sont pas exclusifs l'un de l'autre et qu'il peut y avoir concours idéal d'infractions[374].

II.2.6. Les faits sont-ils compris dans la définition légale de l'infraction ?

Les données et les programmes informatiques sont-ils des choses au sens de l'article 461 du Code pénal ? Sont-ils des choses susceptibles d'être soustraites ?

Traditionnellement, la doctrine considérait que l'article 461 du Code pénal n'était pas applicable aux immeubles et aux choses incorporelles car ceux-ci ne pouvaient être soustraits, la soustraction ne pouvant s'opérer que sur un objet matériel qui a un corps au sens physique du terme[375]. L'article 461 ne s'appliquait dès lors qu'aux choses corporelles définies comme les choses qui, grâce à leurs caractéristiques physiques, pouvaient être touchées.

Pour tenir compte des évolutions scientifiques, il a été admis que le concept de choses corporelles susceptibles d'être soustraites devait être

373 J. -P. BUYLE, L. LANOYE, A. WILLEMS, "Chronique de jurisprudence - L'informatique (1976-1986)", J. T., 1988, p. 119.

374 Voir notamment J. SPREUTELS, "Le vol de données informatiques", *R. D. P.*, 1991, p. 1027.

375 J. NYPELS et J. SERVAIS, "Le code pénal belge interprété", t. III; R. CHARLES, t. XVI, 1961, n°131, 132, 145 et 146.

élargi pour comprendre, non seulement les choses qu'il est permis de toucher, mais aussi celles qu'il est permis de percevoir, que ce soit par l'odorat, la vue ou l'ouïe. Cet élargissement du concept de choses corporelles a permis à la jurisprudence de considérer que le gaz, l'électricité ou les ondes radioélectriques étaient des choses corporelles susceptibles d'être soustraites[376]. Ainsi dans un arrêt du 23 septembre 1981[377], la Cour de Cassation affirme que "l'électricité est susceptible d'appropriation privée. Lorsqu'elle est livrée par celui qui la produit à l'abonné qui la reçoit pour l'utiliser, elle passe par l'effet d'une transmission qui peut être matériellement constatée de la possession du premier dans la possession du second. Elle doit dès lors être considérée comme une chose pouvant faire l'objet d'une soustraction. " En ce sens, la Cour d'appel de Bruxelles a admis qu'il y avait vol en cas de branchement illicite d'un appareil de télévision sur un réseau de télédistribution[378].

La Cour d'appel d'Anvers a été la première juridiction belge à admettre, en 1984, qu'il pouvait y avoir vol de programmes informatiques[379]. Elle a donc considéré que les programmes sont des choses au sens de l'article 461 du Code pénal. Cette jurisprudence a été suivie, entre autres, par le tribunal correctionnel de Bruxelles[380] et la Cour d'appel de Bruxelles[381]. Selon la Cour d'appel d'Anvers, le concept de chose doit être pris dans son sens usuel dans la mesure où celui-ci est conciliable avec le concept de soustraction. La Cour d'appel de Bruxelles précise que le concept de "chose correspondant à des biens meubles susceptibles d'être déplacés ou à des biens matériels susceptibles d'être manipulés physiquement" doit être élargi pour tenir compte de l'évolution de la société. Selon ces juridictions, les programmes sont des choses car ils ont une valeur économique, sont susceptibles d'être transmis et reproduits. Ils font partie du patrimoine du propriétaire du programme original. Font également partie de ce patrimoine les copies du programme original effectuées par le propriétaire. L'auteur de la copie non autorisée, en réalisant celle-ci, s'approprie un élément du patrimoine du propriétaire du programme original. Il fait de même lorsqu'il copie un programme au départ d'une copie du programme original.

En sens contraire, une partie de la jurisprudence[382] et de la doctrine[383] considère que les programmes sont des choses incorporelles ne

376 J. GOEDSEELS, "Commentaire du code pénal belge", II, Bruxelles, 1948 (2ème éd.), n° 2752; H. DE PAGE, "Traité élémentaire de droit civil", t. V, 1952, n° 553.

377 Cass., 23 septembre 1981, *Pas.*, 1982, I, p. 120.

378 Bruxelles, 25 avril 1983, *Pas.*, 1983, II, p. 74.

379 Anvers, 13 décembre 1984, *D. I. T.*, 1986/2, p. 93.

380 Corr. Bruxelles, 31 janvier 1986, Pas., 1986, III, p. 29; Corr. Bruxelles, 14 juin 1993, *J. L. M. B.*, 1993, p. 1131.

381 Bruxelles, 5 décembre 1986, *D. I. T.*, 1987/1, p. 53; Bruxelles, 10 mai 1989, *Pas.*, 1990, II, p. 1.

382 Voir entre autres : Liège, 25 avril 1991, *R. D. P.*, 1991, p. 1013; Corr. Verviers, 4 octobre 1989, *J. L. M. B.*, 1990, p. 70.

pouvant être transmises par la tradition et ne pouvant dès lors être volées. La soustraction ne peut, en effet, s'exercer que sur des objets qui ont un corps au sens physique du terme. Or, "les signaux d'un programme électronique (...) n'ont pas plus d'existence physique d'une idée ou un concept"[384].

II.2.7. La copie illicite est-elle une soustraction au sens de l'article 461 du Code pénal ?

La jurisprudence qui considère que les programmes et les données informatiques sont des choses au sens de l'article 461 du Code pénal, admet également que leur copie non autorisée constitue une soustraction. Cette copie entraîne une appropriation d'un élément du patrimoine du propriétaire du programme original. La notion de soustraction doit s'interpréter en fonction de la nature de la chose qui en fait l'objet et de l'évolution des techniques. La soustraction ne supposerait pas une dépossession physique du propriétaire. Pour qu'il y ait soustraction, il suffit que celui-ci soit privé de sa prérogative essentielle, le droit d'autoriser ou interdire la reproduction. Selon J. Spreutels, "Par la copie, les données tombent véritablement sous sa maîtrise (celle du voleur), avec toutes leurs caractéristiques et leurs intérêts, économiques ou autres. Il (le voleur) peut en disposer librement et leur donner une destination propre. Dupliquer des données, c'est se comporter en propriétaire de celles-ci. (...) Il s'agit d'un acte de disposition sur la chose. S'il reste en possession des données, la situation de leur propriétaire à leur égard sera sensiblement modifiée. Il ne pourra plus exercer de la même façon ses droits sur la chose, car il aura perdu le droit d'usage et de disposition exclusif sur le contenu des données. La valeur, notamment économique, que la donnée représente dans le patrimoine de la victime disparaît, totalement ou partiellement. C'est dans cette mesure que l'on peut dire que chaque copie fait aussi partie du patrimoine"[385].

L'argument contraire est évidemment celui selon lequel il ne peut y avoir soustraction dès lors que le propriétaire garde toujours la possession du programme original, ce qui n'est pas le cas par exemple lors d'une soustraction d'éleetricité.

II.2.8. Falsification de données ou de programmes informatiques

L'article 193 du Code pénal sanctionne le faux en écritures. Dans l'affaire Bistel, la prévention de faux en écritures avait été retenue par le

383 Voir entre autres : B. DE SCHUTTER, "Où en est la fraude informatique ?", Droit de l'informatique - Enjeux - Nouvelles responsabilités, Ed Jeune Barreau Bruxelles, 1993, p 495.

384 Liège, 25 avril 1991, *op. cit*

385 J. SPREUTELS, "Le vol de données informatiques, *op. cit*., p 1058

tribunal correctionnel de Bruxelles à propos de l'utilisation d'un mot de passe n'appartenant pas aux prévenus[386]. Toutefois, la Cour d'appel de Bruxelles[387] rejeta cet argument, estimant que "l'introduction, même d'une manière irrégulière, d'un mot de passe dans le système Bistel ne constitue pas une falsification et que le mot de passe consistant dans un code électronique utilisé par les prévenus ne constitue pas une écriture et, plus précisément, ne constitue pas un système de signes graphiques au sens des articles 193 et suivants du Code pénal".

Dans une affaire mettant en cause une personne ayant manipulé des données afin de reprendre des dossiers à son compte et de créditer plusieurs contrats pour lesquels elle devait procéder à des récupérations, la Cour d'appel de Liège jugea qu'il ne pouvait y avoir faux en écritures au sens de l'article 193 du Code pénal que si la manipulation inscrit les données sur un support matériel. En effet, "pour être punissable, le faux en écritures doit se produire dans un écrit quel que soit le procédé mis en oeuvre pour sa réalisation; (...) les données informatiques appelées par l'opérateur sur l'écran de son ordinateur ne sont que des impulsions magnétiques ne constituant pas des écrits au sens de la loi mais peuvent être l'instrument de leur réalisation."[388]

II.2.9. Lois particulieres

Si le législateur belge n'a pas adopté de dispositions visant de manière spécifique et globale la criminalité informatique, il n'en reste pas moins que diverses législations particulières à certains secteurs traduisent sa prise de conscience certaine des problèmes soulevés.

Il existe tout d'abord des lois qui, bien que ne visant pas spécifiquement le système informatique, exigent la mise en place de mesures préventives de contrôle et de sécurité des traitement de données et qui, par ce biais, concernent également les systèmes informatiques au sens large.

On pense, par exemple, à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, qui met notamment à charge du maître du fichier contenant des données personnelles, des obligations de contrôle ou de restriction d'accès, obligations sanctionnées pénalement[389].

On peut citer, également, la loi sur le registre national des personnes physiques, qui impose aux personnes intervenant dans la collecte le traitement ou la transmission des informations, de prendre « toutes précautions

386 Corr. Bruxelles, 8 novembre 1990, *D. I. T.*, 1991/1, p 51 avec note de C ERKELENS, "Nullem crimen sine lege, nulla poena sine lege : quid?"; *J T*, 1991, p. 11.

387 Bruxelles, 24 juin 1991, *Rev. dr pén.*, 1991, p 340.

388 Liège, 26 février 1992, *J L M. B.*, 1992, p. 1346.

389 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M. B.*, 18 mars 1993, p 5801.

utiles » pour empêcher que celles-ci ne soient déformées, endommagées ou communiquées à des personnes non autorisées à en prendre connaissance[390].

Par ailleurs, le législateur est intervenu, dans le cadre de lois particulières, pour réprimer plus ou moins explicitement certains délits informatiques.

On peut citer, à cet égard, la loi de 1990 relative à l'institution et à l'organisation de la Banque Carrefour de la Sécurité Sociale, qui interdit, entre autres, l'accès ou le maintien non autorisé dans le système informatique, l'introduction, la modification ou la destruction de données ou encore le sabotage de réseaux[391].

Il en est de même, de la loi du 30 juin 1994 sur la protection juridique des programmes d'ordinateur[392]. Celle-ci, qui confère aux créateurs d'un programme original le droit exclusif d'autoriser sa reproduction, réprime pénalement la contrefaçon d'un tel programme. Par ailleurs, elle punit d'une amende de cent à cent mille francs, ceux qui commercialisent ou détiennent à des fins commerciales la copie d'un programme, tout en sachant qu'elle est illicite ou en ayant des raisons de le croire.

La loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques[393], qui réglemente notamment les télécommunications présente un intérêt particulier. En effet, la généralité de ses termes pourrait permettre de poursuivre un grand nombre d'infractions commises via des réseaux tel Internet.

Celle-ci sanctionne en effet le fait : de prendre frauduleusement connaissance de l'existence ou du contenu de signes, de signaux, d'écrits, d'images, de sons, ou de données de toutes natures transmis par voie de télécommunication en provenance d'autres personnes et destinés à celles-ci; de transformer ou de supprimer frauduleusement cette information par n'importe quel procédé technique.

On peut, enfin, se référer à la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes téléphoniques qui interdit, en principe, ces écoutes, si ce n'est dans le cadre d'exceptions strictement délimitées, au bénéfice du juge d'instruction[394]. De par son application à toutes les formes de télécommunication, une telle interdiction vise également la transmission électronique des données entre systèmes informatiques.

390 Loi du 8 août 1983 organisant un registre national des personnes physiques, *M. B.*, 21 avril 1984, modifiée à plusieurs reprises.

391 Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M. B.*, 22 février 1990, p. 3288.

392 Loi du 30 juin 1994 transposant en droit belge la directive européenne du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur, *M. B.*, 27 juillet 1994, p. 19315.

393 Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, *M. B.*, 27 mars 1991, p. 197.

394 Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *M. B.*, 24 janvier 1995, p. 1542.

En conclusion de cette première partie, on peut donc constater que, bien que ne disposant pas de véritable législation spécifique à la criminalité informatique, le droit belge a vocation à réprimer de nombreux délits informatiques, même si ceci est le résultat, tantôt d'une application évolutive du droit pénal traditionnel, tantôt de l'application de quelques dispositions contenues dans des législations particulières éparses.

Nous sommes, en tout état de cause, loin d'une situation de vide juridique, même si certaines questions comme celles de la preuve par exemple, restent problématiques dans certains cas.

III. Internet comme nouveau support d'infractions

III.1. Généralités

« Toute infraction qui peut être commise par émission ou échange d'informations peut être commise par l'Internet »[395]. Ces infractions sont multiples et de natures diverses.

Ces infractions, commises au préjudice d'utilisateurs d'Internet, ou par l'intermédiaire de celui-ci, peuvent être tout d'abord multiples. Les comportements relevant de la diffamation ou de la calomnie, par exemple, de même que les infractions portant atteinte aux mineurs sont susceptibles d'être poursuivies si elles sont commises via Internet.

Nous nous attarderons sur ces deux premiers types d'infractions, particulièrement à l'ordre du jour du fait non seulement de l'actualité législative de certains Etats (voir ci-dessous les développements législatifs au Royaume-Uni, en France et aux Etats-Unis) mais également du fait des comportements eux-mêmes constatés sur Internet. Toutefois, on mentionnera que d'autres contenus illégaux peuvent donner lieu à des poursuites, dont l'incrimination est prévue dans le Code pénal ou dans des législations particulières.

On peut songer ainsi aux atteintes à la sécurité de l'Etat (drogue, terrorisme, etc.). Sur le plan des législations particulières, on renverra par exemple aux actes racistes ou xénophobes prohibés par la loi du 30 juillet 1991, ou à l'inflation de textes législatifs particuliers qui sanctionnent pénalement le non respect de leurs dispositions. Ces législations ont également vocation à s'appliquer, vu la généralité de leurs termes, à des communications sur Internet. On peut citer par exemple la loi du 14 juillet 1991 relative aux pratiques du commerce, à l'information et à la protection des consommateurs, ou encore les dispositions en matière d'expositions, d'offres et de vente de titres ou valeurs mobilières[396].

Ensuite, les comportements observés sur Internet peuvent être de nature diverse. On conçoit ainsi que la mise à disposition d'un site Web est d'une nature différente que l'envoi d'un courrier électronique. Ne faudrait-il pas appliquer aux sites Web le système de la responsabilité en cascade existant en matière de presse écrite ? On rappellera que les poursuites, l'instruction et le jugement d'un délit de presse — par exemple la diffamation — se déroulent comme en matière criminelle, soit à l'intervention de la Cour d'Assises. En pratique, on ne poursuit dès lors pratiquement plus les délits de presse, ce qui fait dire à certains que la presse écrite bénéficie ainsi d'une impunité pénale quasi totale. E. Montero livre une analyse de la question dans son exposé. Nous nous contenterons d'y renvoyer, étant donné les limites du nôtre.

Par ailleurs, il semble de bon sens de faire une distinction entre les message émis avec une certaine publicité et l'envoi de messages à une personne déterminée. Alors que l'envoi de messages de manière purement privée relève du secret des correspondances, nous verrons plus loin que la publicité donnée à un message électronique confère à celui-ci une nature particulière à laquelle correspondent des règles spécifiques en matière pénale. On concédera cependant qu'il n'est pas toujours aisé de tracer la limite entre les infractions de diverse nature dans le cadre d'Internet.

395 Jean-François Chassaing, L'Internet et le droit pénal, Recueil Dalloz-Sirey, 38ème Cahier, p. 332.

396 Arrêté royal n° 185 du 9 juillet 1935. Voir, sur ce point : J. -P. BUYLE, O. POELMANS, Internet : quelques aspects juridiques, *DIT*, 1997, à paraître

III.2. Illustration en droit belge : la diffamation et la pornographie enfantine

Il nous a semblé judicieux de prendre la diffamation et la calomnie, d'une part, et la pornographie enfantine, d'autre part, pour illustrer la problématique de l'application du droit pénal à Internet. En tant que nouveau moyen d'exercice de la liberté d'expression, Internet est soumis aux mêmes limites que les moyens plus traditionnels d'exercice de celle-ci.

III.2.1. La diffamation et la calomnie

Des informations transmises sur Internet pourraient être poursuivies sur la base des dispositions réprimant la calomnie ou encore la diffamation, réprimées à l'article 443 du Code Pénal.

Celui-ci énonce :

> « Celui qui, dans les cas ci-après, a méchamment imputé à une personne un fait précis qui est de nature à porter atteinte à l'honneur de cette personne ou à l'exposer au mépris public, et dont la preuve légale n'est pas rapportée, est coupable de calomnie lorsque la loi admet la preuve du fait imputé, et de diffamation lorsque la loi n'admet pas cette preuve ».

Il est particulièrement intéressant de se pencher sur les conditions de réalisation qu'une telle infraction implique. L'article 444 du Code Pénal exige en effet que des propos, pour être constitutifs de calomnie ou de diffamation, aient été tenus de manière publique.

Deux formes de publicité doivent plus particulièrement retenir notre attention s'agissant d'appliquer cet article à Internet.

D'une part, selon l'article 444 alinéa 5, la publicité peut être réalisée par « *des écrits imprimés ou non, des images ou des emblèmes affichés, distribués ou vendus, mis en vente ou exposés aux regards du public* ».

On pourrait donc, semble-t-il, appliquer cette disposition à des applications de type sites Web, puisqu'il s'agit bien là d'écrits ou d'images exposés aux regards du public. De même, cette disposition nous paraît même pouvoir être appliquée dans le cadre de certains groupes de discussion dits publics selon les distinctions effectuées en matière de services offerts via Internet. En effet, le fait de mettre à disposition de tout qui prend connaissance des informations reprises sur un site particulier, accessible par la composition d'une adresse donnée sans autre condition, nous semble correspondre suffisamment à la notion d'exposition au regard du public exigée par l'article 444.

La solution pourrait être plus controversée s'agissant des messageries publiques, étant donné les démarches actives que doit accomplir l'utilisateur d'Internet pour accéder à cette messagerie. Néanmoins, dans ce dernier cas, l'article pourrait fournir une base légale légitime pour la poursuite des personnes responsables de propos calomnieux ou diffamatoires. L'article 444 sanctionne en effet également, in fine, la calomnie ou la diffamation représentées « *par des écrits non rendus publics, mais adressés ou communiqués à plusieurs personnes* ». Les groupes de discussion ou les messages envoyés à plusieurs destinataires pourraient se voir appliquer cette disposition.

On remarquera que le texte de l'article 444 n'exige pas le caractère imprimé des écrits, ce qui devrait permettre de couper court aux controverses sur la question de savoir si des pages Web ou des messages peuvent y être assimilés. Ceci sans compter que la grande majorité des textes circulant sur le réseau peuvent être imprimés par leur visiteur ou destinataire.

III.2.1. La pornographie enfantine

Un reproche lancinant exprimé à l'encontre d'Internet est qu'il facilite la diffusion de contenus à caractère pornographique, en particulier concernant la pornographie enfantine[397].

La question de la pornographie se pose en des termes divers. Toutes les communications à caractère pornographique ne sont pas susceptibles d'être poursuivies ou ne sont pas poursuivies dans les faits. La notion de contrariété aux bonnes moeurs est évolutive et est essentiellement développée par les juges[398]. Par exemple, la simple détention ou l'échange

397 Voir par exemple l'article de presse cité dans l'introduction de la présente contribution

398 Notamment par l'interprétation de l'article 383 du Code pénal, appliqué entre autres aux images des vidéocassettes, qui énonce : « Quiconque aura exposé, vendu ou distribué des chansons, pamphlets ou autres écrits imprimés ou non, des figures ou des images contraires aux bonnes moeurs, sera condamné à un emprisonnement de huit jours à six mois et à une amende de vingt-six à cinq cents francs. ( ) ».

d'images pornographiques électroniques entre adultes et n'impliquant que des adultes consentants ne seront pas poursuivies. La pornographie « tolérée » sur Internet pose plutôt, dans cette optique, des questions quant à l'accessibilité des mineurs[399]. Nous reviendrons sur cette question à l'occasion de l'examen des solutions techniques analysées à la fin du présent exposé.

Par contre, certaines formes de pornographie sont interdites purement et simplement. C'est le cas de la pornographie impliquant des mineurs (pornographie enfantine). La question se pose, dès lors, de l'applicabilité des dispositions pertinentes à la communication sur Internet.

Il nous faut examiner dans ce cadre les articles 383 bis et 383 quinquies du Code Pénal insérés par deux lois de 1995 (du 13 avril et du 27 mars).

L'article 383 bis vise explicitement la pornographie enfantine. Son texte énonce :

> « §1er. Sans préjudice de l'application des articles 379 et 380 bis, quiconque aura exposé, vendu, loué, distribué ou remis des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs âgés de moins de 16 ans ou les aura en vue du commerce ou de la distribution, fabriqués ou détenus, importés ou fait importer, remis à un agent de transport ou de distribution, sera puni de réclusion et d'une amende de cinq cent francs à dix mille francs.
>
> §2. Quiconque aura sciemment possédé les emblèmes, objets, films, photos, diapositives ou autres supports visuels visés sous le § 1er sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent francs à mille francs.
>
> §3. L'infraction visée sous le paragraphe 1er, sera punie des travaux forcés de 10 ans à 15 ans et d'une amende de cinq cent francs à cinquante mille francs, si elle constitue un acte de participation à l'activité principale ou accessoire d'une assoeiation, et ce, que le coupable ait ou non la qualité de dirigeant.
>
> (...)[400]. »

On remarquera que la simple possession (consciente) de matériel est réprimée par cet article. Le champ d'application de cette disposition, comme on le constate, est assez étendu. Il nous semble que la généralité des termes employés permet l'application de cette disposition à la porno-

399 Cette distinction se retrouve dans de nombreux Etats membres de l'Union européenne. Voir sur cette distinction, notamment, le Livre vert de la Commission européenne du 16 Octobre 1996 sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information (COM (96) 483, notamment p. 15.

400 L'article 379, instauré également par la loi de 1995, énonce : « Quiconque aura attenté aux moeurs en excitant, favorisant ou facilitant, pour satisfaire les passions d'autrui, la débauche, la corruption ou la prostitution d'un mineur de l'un ou l'autre sexe, sera puni de réclusion et d'une amende de cinq cents francs à vingt-cinq mille francs. (...) »

graphique enfantine sur Internet, quel que soit le service d'Internet considéré.

D'autre part, une loi du 27 mars 1995 a inséré un article 380 quinquies, qui condamne la publicité pour des services à caractère sexuel impliquant des mineurs :

> « §1er. Sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de deux cents francs à deux mille francs quiconque, quel qu'en soit le moyen fait ou fait faire, publie, distribue ou diffuse de la publicité, de façon directe ou indirecte même, en en dissimulant la nature sous des artifices de langage, pour une offre de serviee à caractère sexuel ayant un but lucratif direct ou indirect, lorsque cette publicité s'adresse spécifiquement à des mineurs ou lorsqu'elle fait état de services proposés soit par des mineurs, soit par des personnes prétendues telles.
>
> La peine sera d'un emprisonnement de trois mois à trois ans et d'une ameude de trois cents francs à trois mille francs lorsque la publicité visée à l'article 1er a pour objet ou pour effet, direct ou indirect de faciliter la prostitution ou la débauche d'un mineur ou son exploitation à des fins sexuelles.
>
> § 2. Sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent francs à mille francs, quieonque, quel qu'en soit le moyen fait ou fait faire, publie, distribue ou diffuse de la publicité, de façon directe ou
>
> indirecte, même en en dissimulant la nature sous des artifices de langage, pour une offre de services à caractère sexuel ayant un but lucratif direct ou indirect, lorsque ces services sont fournis par un moyen de télécommunication.
>
> (...). »

Contrairement à l'article 383bis, c'est ici la publicité pour des services à caractère sexuel qui est condamnée et non plus la communication à caractère pornographique. Les termes sont ici également suffisamment larges pour englober la publicité pour l'offre de services sur Internet, puisque le paragraphe 1er incrimine la publicité « quel qu'en soit le moyen ».

On remarquera également que cette disposition vise non seulement la publicité pour des services impliquant des mineurs mais également la publicité dirigée spécifiquement vers les mineurs.

On notera, enfin, que la publieité pour l'offre de services fournis eux-mêmes par télécommunication est explicitement prévue au paragraphe 2 de l'article[401] Les services eux-mêmes, s'ils impliquent des mineurs, devront être poursuivis sur la base de l'article 383his précité. Internet relevant par essence de la télécommunication, il n'est pas douteux que ce genre de services rentre bien dans le champ d'application de cette disposition.

401 On rappellera le contexte particulier de cet article, à savoir les messageries roses et non, à proprement parler les applications liées à Internet.

IV. Questions soulevées par l'application du droit pénal

D'autres questions complexifient cependant quelque peu l'appréhension des infractions commises par le biais du réseau des réseaux.

IV.1. La détermination de la loi applicable et du juge compétent

Internet ne connaît pas les frontières des Etats, et ceci pourrait constituer peut être le point le plus problématique sur le plan juridique. Bien que le droit belge ne soit pas sans ressource à cet égard, la coopération internationale est pour le moins lacunaire s'agissant de régler les conséquences du caractère par essence transnational de la communication via Internet.

IV.1.1. La détermination de la loi applicable et du juge compétent

Par sa caractéristique transnationale, le réseau Internet permet par exemple à tout personne, utilisant son ordinateur dans un pays ticrs, de mettre à disposition des pages Web, qui pourront être consultées à tout autre endroit dans le monde, pourvu que l'on dispose des facilités informatiques et de télécommunication nécessaires. Quid, à titre purement illustratif, si un utilisateur belge « visite » un site Web hébergé sur un serveur situé aux Etats-Unis et présentant des pages à caractère raciste ?

La détermination de la loi applicable et du juge compétent, contrairement à la situation rencontrée sur le plan du droit civil[402], ne pose pas de difficultés insurmontables en droit belge, comme d'ailleurs dans la plupart des Etats européens.

L'article 3 du Code Pénal énonce en effet :

> « L'infraction commise sur le territoire du royaume, par des Belges ou par des étrangers, est punie conformément aux dispositions des lois belges ».

Bien qu'aucune disposition ne vienne déterminer ce que l'on entend par « infractions commises sur le territoire du Royaume », la jurisprudence est constante et considère, en application de la théorie dite de l'ubiquité, que le juge belge est compétent lorsqu'un des éléments constitutifs de l'infraction est localisé en Belgique[403]. Il s'agit bien, en l'espèce, d'un

402 Voir l'exposé consacré à ce sujet.

403 Voir par exemple : Cass. 8 novembre 1930, *Pas.*, 1931, I, 8. Cass. 18 novembre 1957, Pas., 1958, I, 285.

« aménagement du principe de la stricte territorialité du droit pénal »[404] qui n'est d'ailleurs pas propre à la Belgique[405].

Cette théorie de l'ubiquité a été par exemple appliquée en matière de radiodiffusion. Il a été ainsi jugé : « Attendu dès lors qu'à juste titre les faits ainsi circonscrits sont qualifiés de calomnie (...); Que réalisés par voie de radiodiffusion, ils sont supposés accomplis en tout lieu où pareille diffusion a pu être reçue ou entendue, l'élément constitutif de l'infraction, l'imputation publique, ayant été réalisée de cette manière; Que l'infraction est donc supposée avoir été commise principalement sur le territoire de la Belgique (...) » [406].

Il nous semble envisageable d'appliquer cette solution dans le cas d'un destinataire d'un service Internet fourni via l'étranger, bien que, sur un plan strictement technique, les opérations de radiodiffusion et de « diffusion » sur Internet soient différentes[407]. Etant donné la possibilité de diffusion ou de réception des messages Internet partout en Belgique, les juges de tous les arrondissements judiciaires sont done par hypothèse compétents.

Si cette situation peut convenir au juge et à l'utilisateur belge d'Internet, on fera toutefois remarquer que ce principe de compétence aboutit à des conflits positifs de compétence territoriale. Il en résulte des situations complexes pour les fournisseurs de services et autres intermédiaires qui, potentiellement, peuvent ainsi être poursuivis devant de nombreuses juridictions des différents Etats appliquant ee principe et devraient dès lors, en théorie, respecter les législations de tous les Etats où le service peut être reçu...

Dans le eas où cette théorie ne pourrait être appliquée, c'est-à-dire si l'on considère qu'aucun élément constitutif de l'infraction n'a été commis sur le territoire belge, c'est l'article 4 du Code pénal ainsi que le chapitre II du Code d'instruction criminelle qui fondent la compétence territoriale, assortie de conditions spécifiques telles que le principe Ne bis in idem inscrit à l'article 13 du C.i.cr. [408]. Ce dernier principe a été modalisé par

404 L'expression est de J. SPREUTELS, in : J. SPREUTELS, Vers un droit pénal international des affaires, *JT*, 1981, p. 185.

405 Voir par exemple, en France, l'article 113-2 du Code pénal. A propos d'Internet et de la compétence du juge pénal français, Michel VIVANT conclut « Le « phénomène réseau » n'engendre aucune difficulté singulière » (Michel VIVANT, Cybermonde : Droits et droits des réseaux, la Semaine Juridique, 1996, I, 3969, p. 405 et suivantes).

406 Bruxelles, 5 décembre 1991, *JT*, 1992, p. 387 et suivantes, note F. Jongen; voir également Liège (civ.), 15 octobre 1990, JLMB, 1991, p. 659 et suivantes. La première décision citée fait elle-même référence à une décision française de 1979 (Cass. Fr., 8 octobre 1979, Rev. Sc. Crim., 1980, p. 987).

407 J. P. BUYLE et O. POELMANS considèrent au contraire que les situations sont techniquement identiques, mais arrivent à la même conclusions. Voir J.-P. BUYLE, O. POELMANS, "Internet : quelques aspects juridiques", *D.I.T.*, 1997, à paraître.

408 Les conditions d'application du principe Ne bis in idem étant cependant strictes, le risque de voir poursuivre ou de juger une personne plusieurs fois est réel. Sur la portée et l'interprétation de cet article 13, voir : G. VERMEULEN, Het beginsel Ne Bis In Idem in het Internationaal strafrecht - Een evaluatie van de nationale en verdragsrechtelijke waarborgen in het strafrechtsverkeer met onze buurlanden, Panopticon, 1994, p. 217 et suivantes.

voie de conventions internationales, bilatérales ou multilatérales, dont la grande majorité, malheureusement, n'ont pas force de loi en Belgique[409].

IV.1.2. La coopération internationale en matière pénale

Il ne s'agit pas ici d'analyser l'ensemble des instruments réglementaires visant la coopération en matière pénale, élaborés de manière bilatérale ou au sein du Conseil de l'Europe, de l'Union européenne, du Groupe Schengen ou du Bénélux[410]. Ceci dépasserait l'objet de notre exposé. Ces traités concernent par exemple la poursuite des infractions ou la validité des décisions en matière répressive[411]. Par ailleurs, la plupart n'ont aucune valeur contraignante pour la Belgique, qui n'en a pratiquement ratifié aucun.

D'autre part, les traités multilatéraux concernent pour la plupart la coopération entre Etats européens. En d'autres termes, la coopération en matière répressive entre la Belgique et d'autres pays que les Etats européens échappe à ces instruments, bien que certaines conventions bilatérales aient été élaborées.

Ces lacunes ont bien entendu un impact certain, notamment au plan de l'exécution des décisions pénales intervenues en Belgique à l'encontre de personnes résidant à l'étranger. Il faut bien reconnaître, cependant, que cette question est néanmoins d'ordre plus politique que strictement juridique, puisque certains instruments existent dès à présent. Elle n'est d'ailleurs pas propre à Internet. Il n'en reste pas moins que la globalisation et l'importance croissante de la communication électronique dans nos sociétés confèrent à la coopération policière et judiciaire un caractère particulièrement urgent.

Cependant, ainsi que le fait remarquer Michel Vivant, dans un article récent[412], l'effet d'une condamnation pénale à l'encontre d'un étranger résidant hors de Belgique, même si son exécution ne peut avoir lieu en pratique, n'est pas négligeable pour autant.

On rappellera tout d'abord qu'une incrimination pénale porte en elle un certain effet préventif. On objectera que cet effet n'est certes pas le même dans le cas où le comportement incriminé en Belgique ne l'est pas dans l'Etat de l'émetteur du contenu répréhensible. Il se trouve cependant

409 Ibidem.

410 Voir, sur le plan européen : F. THOMAS, De Europese rechsthulpverdragen in strafzaken, Gand, Story-Scientia, 1980, ainsi que les nombreuses références citées par G. VERMEULEN, *op. cit.*, p. et suivantes.

411 Voir notamment le Traité du 13 novembre 1991 signé entre les Etats membres de l'Union européenne relatif à l'exécution des décisions étrangère rendues en matière répressive.

412 Michel VIVANT, Cybermonde : Droits et droits des réseaux, la Semaine Juridique, 1996, I, 3969, p. 406.

que de nombreuses infractions poursuivies en Belgique le sont également dans d'autres Etats, même si les conditions légales divergent parfois sensiblement[413]. Par ailleurs, une condamnation pénale a un effet certain de par son existence, notamment par son effet stigmatisant.

Ces deux éléments peuvent bien sûr freiner les initiatives de certains. Il nous semble, par ailleurs, que l'effet doit également être envisagé sur le plan de la complicité des intermédiaires de la communication. Ainsi que nous le verrons ci-dessous[414], la complicité d'un intermédiaire — on pense en particulier aux fournisseurs d'accès et aux serveurs — pourrait plus facilement être retenue lorsque l'intermédiaire concerné connaît ou devrait connaître le comportement délictueux des personnes dont il transmet ou héberge les informations.

Par ailleurs, à une action pénale peut être associée une action civile en dommages et intérêts. Or, ces décisions sont plus facilement exécutées à l'étranger, vu l'existence des conventions internationales qui sont, elles, en vigueur[415].

IV.2. L'anonymat

Dans le cadre de la communication sur Internet se pose la question de l'identification de ses utilisateurs. L'émetteur d'un message peut ne pas vouloir décliner son identité lorsqu'il demande ou donne des informations délicates, que ce soit sur le plan de son état de santé, sur ses opinions politiques ou ses convictions religieuses ou encore ses préférences sexuelles.

Cette « anonymisation » est pratiquée dans le cadre d'Internet, du moins du point de vue du destinataire des messages. Il reste que l'auteur d'un contenu doit également assumer la responsabilité d'un contenu éventuellement préjudiciable. Sur ce point, la Commission européenne, qui a adopté en octobre 1996 une communication sur le contenu illégal et préjudiciable sur Internet[416], recommande une solution qui mérite l'attention, et qui correspond à une réelle crainte des autorités judiciaires.

La Commission recommande à cet égard le principe de la « traçabilité » ou principe d'identification légale des utilisateurs d'Internet. Un utilisateur souhaitant conserver l'anonymat devrait confier aux réexpéditeurs anonymes les données qui l'identifient. Ces réexpéditeurs devraient remettre ces données à la demande des autorités policières ou judiciaires,

413 Ainsi, par exemple, l'âge des personnes en matière de protection des mineurs divergent parfois sensiblement d'un Etat à l'autre, même au sein des pays européens.

414 Voir notamment l'arrêt du tribunal fédéral suisse mentionné ci-après

415 Voir sur ce point la contribution de E. MONTERO.

416 Communication de la Commission européenne du 16 octobre 1996 « Contenu illégal et préjudiciable sur Internet », Com (96) 487 final, pp. 14-16.

dans le respect des dispositions législatives et réglementaires en vigueur en matière de protection des données personnelles. Si ce principe n'est en réalité que l'expression de règles préexistantes, la Commission entend cependant promouvoir le développement de solutions techniques appropriées ainsi que la coopération nécessaires à l'efficacité de ces règles[417].

IV.3. La responsabilité

La multiplicité des acteurs de la communication sur Internet et la superposition des rôles qu'ils peuvent endosser tour à tour rendent plus complexe la détermination de leur responsabilité respective lors de la commission d'infractions.

On peut distinguer différents acteurs de la communication sur Internet, notamment l'opérateur de réseaux, le fournisseur d'accès, le serveur (qui peut héberger des sites mais également gérer des groupes de discussion ou des messageries publiques), le fournisseur de contenu (auteur ou éditeur). On notera encore que le fournisseur de services peut également proposer sur un site particulier des liens hypertexte vers d'autres sites, etc. Les possibilités sont multiples et ont déjà été décrites dans d'autres exposés.

Si l'on exclut l'application du système de responsabilité en cascade de la presse écrite[418], qui ne correspond pas vraiment aux caractéristiques d'Internet[419], les règles pénales de la complicité peuvent fournir certains éléments de réponse à la question de la détermination des acteurs responsables[420].

Le Code Pénal belge (articles 66 à 69) exige deux conditions pour établir la complicité :

— la conscience de participer à une infraction déterminée;
— la volonté d'arriver au résultat recherché.

Si l'opérateur de télécommunications se cantonne dans son rôle de simple point d'accès à Internet, il ne devrait en principe pas être inquiété. Par contre, la responsabilité des fournisseurs d'accès et autres centres serveurs pourraient être mise en cause dans certains cas, pour autant que

417 Commission européenne, *op. cit*, p. 16.

418 Voir sur ce point la contribution de E. MONTERO et le rapport français de la Mission Interministérielle sur l'Internet présidée par Isabelle Falque-Pierrotin, Paris, 1996, p. 56 et suivantes.

419 Etant donné le caractère non imprimé de l'information et le nombre exponentiel de « contenus » que les intermédiaires concernés traitent

420 Voir J.-P. BUYLE, O. POELMANS, "Internet : quelques aspects juridiques", *D. I. T.*, 1997, à paraître.

l'infraction soit commise dans le cadre d'un service accessible au public[421].

En effet, si le serveur ou fournisseur d'accès obtient des informations spécifiques sur le contenu illicite de messages, soit par ses propres moyens, soit par des tiers et ne prend pas les mesures appropriées pour y mettre fin, on peut considérer qu'un niveau de connaissance suffisant est atteint pour l'application des règles de la complicité pénale. Une telle solution nous semble envisageable également, s'agissant de sites renvoyant par des liens de type hypertexte à des contenus illicites.

Une décision suisse a été rendue en ce sens. Dans son arrêt "du 156"[422], le tribunal fédéral suisse a constaté que les responsables des P. T. T. de l'introduction d'un service de type télékiosque se rendaient coupables de complicité de pornographie, dès lors qu'ils fournissaient les prestations nécessaires à l'exploitation du télékiosque tout en sachant qu'il servait à diffuser des enregistrements pornographiques accessibles, notamment à des jeunes de moins de 16 ans, ce qui leur avait été signalé par le Ministère Public.

Le rôle des tiers (en cause, le tiers étant le Ministère Public lui-même), par l'information qu'ils peuvent donner sur le caractère répréhensible des messages, est central, dans cette optique.

On pourrait toutefois objecter, s'agissant de services accessibles au public, qu'un contrôle systématique du contenu des messages véhiculés est totalement irréaliste. Pour ne citer qu'un seul chiffre, on peut évaluer que le simple trafic d'informations au sein des quelques 17. 000 groupes de discussions d'Internet présentent un volume de textes estimé à plusieurs milliers de livres[423].

Ainsi, la Cour de Cassation française a-t-elle acquitté en 1990 un centre serveur télématique hébergeant une messagerie rose incitant à la débauche, invoquant l'impossibilité pour celui-ci de contrôler le contenu des messages des nombreux services qu'il hébergeait[424].

Sur le plan législatif, on notera trois initiatives de responsabilisation relative des fournisseurs d'accès à Internet, dont deux ont toutefois partiellement échoué.

421 Les communications privées sont protégées par le secret de la correspondance.

422 ATF 121 IV 109 ss.

423 Voir les chiffres cités par le rapport d'un groupe interdépartemental sur des questions relevant du droit pénal, du droit de la protection des données et du droit d'auteur suscitées par Internet, rapport pour l'Office fédéral de la Justice suisse, mai 1996, p. 5.

424 Cass. Crim. 15 novembre 1990, *DIT*, 1990/4.

Au Royaume-Uni, le "Defamation Act" adopté en juillet 1996 prévoit que peuvent être invoqués par le défendeur, comme moyens de défense dans une procédure en diffamation, entre autres, les trois éléments cumulatifs suivants :

— il n'est pas l'auteur ou éditeur du propos diffamatoire ("he was not the author, editor or publishor of the statement complained of");
— il a pris toute les précautions raisonnables pour sa publication ("he took reasonable care in relation to its publication");
— il ne savait pas et n'avait pas de raison de savoir que l'on provoquerait ou contribuerait à la publication d'un tel propos ("he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement").

La loi précise ensuite que n'est pas considéré comme auteur ou éditeur celui qui agit uniquement comme opérateur ou fournisseur d'accès à un système de communications par le moyen duquel le propos a été transmis, ou rendu accessible, par une personne sur lequel il n'avait pas de contrôle effectif. Ne sera également pas considéré comme auteur ou éditeur celui qui est uniquement impliqué dans le traitement, la copie, la distribution ou la vente d'un support électronique sur lequel se trouve le propos diffamatoire. Il en est de même de celui dont le rôle est uniquement d'opérer ou de fournir l'équipement, le système ou le service par lequel le propos est extrait, copié, distribué ou rendu accessible sous forme électronique[425].

Il est intéressant de noter que si le fournisseur d'accès est considéré par la juridiction saisie comme étant un "publisher", ce qui a été le cas dans certaines décisions rendues aux Etats-Unis[426], ces moyens de défense ne pourront être invoqués.

Par contre, en France, l'amendement relatif à la responsabilité pénale des fournisseurs d'accès proposé par le Ministre des Télécommunications dans le cadre de la révision des réglementations sur les télécommunications n'a pas été adopté par l'Assemblée parlementaire. Il posait le principe de la non responsabilité pénale des fournisseurs d'accès pour autant

425 "A person shall not be considered the author, editor or publisher of a statement if he is only involved :

(c) in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form;

(e) as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control. "

426 Voir entre autres : Stratton-Oakmont, Inc. v. Prodigy Service Co, NY Sup Ct, 24 mai 1995. Toutefois, dans un souci de contourner cette jurisprudence, le "Communication Decency Act" dont certaines dispositions sont contestées devant les juridictions américaines (voir ci-dessous), prévoit que les fournisseurs d'accès ne peuvent être considérés comme éditeurs ("publisher") de matériaux fournis par d'autres fournisseurs de contenu et qu'aucun fournisseur d'accès ne peut être tenu civilement responsable d'une action volontairement entreprise de bonne foi afin de limiter l'accès à des matériaux considérés comme étant obscènes, excessivement violents, etc. même si ces matériaux sont protégés par la Constitution américaine.

que ceux-ci proposent à leurs clients un moyen technique leur permettant de restreindre l'accès à certains services ou de les sélectionner et que le service n'ait pas fait l'objet d'un avis défavorable du Comité supérieur de la Téléinatique.

Toutefois, la responsabilité du fournisseur d'accès pouvait dans tous les cas être mise en cause dès lors qu'il était établi qu'il avait "en connaissance de cause, personnellement commis l'infraction ou participé à sa commission".

Le Conseil Constitutionnel français a émis des objections quant à cet amendement, notamment parce qu'il permettait en quelque sorte au Conseil Supérieur de la télématique de décider de la responsabilité pénale du fournisseur. A toutefois été adoptée l'obligation imposée à tout fournisseur d'accès à un service de communication audiovisuelle de proposer un moyen technique de filtrage.

Enfin, aux Etats-Unis, le "Communication Decency Act", adopté en février 1996 sanctionne pénalement tout qui, sciemment, est à l'origine de la transmission de commentaires, demandes, suggestions, propositions, images ou autres communications obscènes et indécentes[427]. Les moyens de défense qui peuvent être invoqués sont entre autres :

— le fait d'avoir pris, de bonne foi, des mesures raisonnables, effeetives et appropriées pour empêcher ou limiter l'accès aux mineurs à des communications indécentes;
— le fait d'avoir restreint l'accès à de telles communications par l'exigence d'une carte de crédit, d'un code secret ou d'un numéro d'identification pour personnes adultes.

Cependant, par une « preliminary injunction » du 11 juin 1996, la "District Court" de Pensylvannie a suspendu ces dispositions, dans une affaire ACLU v. RENO, en considérant qu'elles étaient contraires au premier amendement de la Constitution américaine qui garantit la liberté d'expression. Un des arguments fut, en substance, que la restriction à la liberté d'expression découlant des obligations susmentionnées était exagérée. Entre autres, parce que toutes les organisations, même non commerciales, n'avaient pas les moyens de disposer disposent de ces moyens techniques.

La preliminary injunction énonce ensuite que : « (...)As a practical matter, non-commercial organizations and even many commercial organizations using the Web would find prohibitively expensive and burdensome to engage in the methods of age verification proposed by the government, and that even if they could attempt to age verify, there is little assurance that they could successfully filter our minors ».

427 Lorsque cette communication n'est pas destinée à des mineurs de moins de 18 ans, le simple fournisseur d'accès n'est pas tenu responsable.

Le texte continue : « (...) Many speakers who display arguably indecent content on the Internet must choose between silence and the risk of prosecution ».

Sans entrer dans le détail, il est intéressant de noter la différence d'approche entre le Conseil constitutionnel français et la juridiction américaine, puisque cette dernière base essentiellement son argumentation sur le premier amendement garantissant la liberté d'expression, alors que la première raisonnait plutôt, oserions-nous dire, en termes de « compétences ». Quoi qu'il en soit, l'on perçoit dès à présent l'importance que peuvent revêtir le développement et l'utilisation de systèmes techniques de filtrage de certains contenus, sur lesquels nous revenons dans nos conclusions.

V. Conclusions : des solutions complémentaires ?

On aura pu constater, lors de ce bref examen du droit pénal que, bien que ne disposant pas de véritable législation spécifique à la criminalité informatique, le droit belge a vocation à réprimer de nombreux délits informatiques commis par le biais d'Internet, même si ceci est le résultat, tantôt, d'une application évolutive du droit pénal traditionnel, tantôt de l'application de quelques dispositions contenues dans des législations particulières éparses.

Internet peut ensuite servir de support, au même titre que de nombreux autres moyens de communication, à une « criminalité d'expression », ce qu'un récent rapport suisse décrivait comme les « délits d'opinion », entendus au sens large[428]. Nous avons vu, en particulier à travers deux exemples, que le droit pénal belge n'est pas non plus sans ressource face à cette nouvelle forme de criminalité.

Toutefois, certaines caractéristiques d'Internet, en particulier sa nature transnationale, posent fondamentalement question. Nous avons constaté que cette question est bien plus d'ordre politique que juridique. Or, on connaît l'espoir, tant en termes socio-économiques que de développement culturel, fondé sur Internet et, de manière plus générale, sur la société de l'information[429]. Dans ce contexte, il paraît essentiel de pouvoir garantir un niveau suffisant de protection des citoyens et de l'intérêt public, si l'on veut favoriser la confiance en Internet[430].

Que peut-on proposer comme solution à moyen et à long terme pour garantir les droits de chacun sur Internet ? Nous nous proposons d'en aborder trois catégories, souvent mises en avant, notamment par les institutions de l'Union européenne[431] : la coopération, voire l'harmonisation au plan international, l'autoréglementation et les solutions techniques.

428 Rapport pour l'Office fédéral de la Justice Suisse, *op. cit.*

429 Voir, à titre d'exemple, la Résolution du Conseil de l'Union européenne (96/C 376/01) du 21 novembre 1996, JOCE n° C 376, 12 décembre 1996. Voir également le Livre vert de la Commission sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information du 16 octobre 1996, COM (96) 483, ainsi que la Communication de la Commission « Contenu illégal et préjudiciable sur Internet » du 16 octobre 1996, COM (96) 487.

430 Dans la résolution précitée, le Conseil de l'Union européenne devait aussi reconnaître que la ditribution de matériel illicite affectant l'ordre public et la moralité pourrait hypothéquer la confiance et l'acceptation de la nouvelle « société de l'information ».

431 Voir par exemple le Livre vert de la Commission européenne sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'informations, ainsi que la Communication de la Commission sur les contenus illégaux et préjudiciables sur Internet, tous deux précités.

V.1. La coopération, voire l'harmonisation au plan international

Il est certain que nombre de problèmes peuvent être réglés, en théorie, si les Etats s'entendent sur des standards communs de répression de la criminalité. Certains des efforts produits dans ce sens, notamment au sein du Conseil de l'Europe, ont été mentionnés ci-dessus. On connaît cependant les limites d'une telle coopération intergouvernementale. En particulier s'agissant de droit pénal, l'attachement des Etats à leur souveraineté et aux principes de territorialité du droit pénal, notamment, conditionnent pour une grande part la politique internationale des gouvernements. La réserve exprimée par les Etats est d'ailleurs légitime dans bien des cas, puisqu'il y va de conceptions différentes de notions aussi essentielles que la liberté d'expression ou la protection de l'ordre public et des bonnes moeurs.

Dans un tel contexte, la recherche de standards communs, louable en soi, risque souvent d'aboutir à des solutions de compromis, à des « plus petits communs dénominateurs » dont l'efficacité est malheureusement disproportionnée au regard des efforts diplomatiques fournis.

On mentionnera à cet égard la récente proposition du Ministre français Fillon, présentée à l'O. C. D. E. en 1996 et tendant à l'élaboration d'une charte sur Internet. Dans cette proposition, les Etats reconnaissent ainsi que, « en raison du caractère intrinsèquement international du réseau Internet, sa réglementation soulève des problèmes qui bénéficieront grandement d'une approche harmonisée. Ils s'engagent donc à coopérer afin de rapprocher leurs pratiques nationales relatives à Internet »[432].

Si ces efforts ne sont pas totalement vains, ils devraient, à notre avis, être privilégiés dans les enceintes internationales regroupant des Etats partageant des conceptions suffisamment comparables des intérêts à protéger. Les pays européens, à cet égard, partagent bien sûr des conceptions de la protection de l'intérêt général relativement proches les unes des autres[433]. On n'oubliera pas non plus que l'Union européenne elle-même ne dispose pas de compétence particulière en matière d'harmonisation du droit pénal.

Il reste que, si des solutions sont envisageables, à long terme, au niveau de l'Union européenne, il faut toutefois reconnaître qu'Internet ne connaît pas plus les frontières de l'Union européenne que celles des Etats membres.

432 Document disponible sur le site Internet du gouvernement français (gouv fr/français/activ/techno/charteint.htm).

433 Voir en matière de conceptions de la liberté d'expression, l'analyse comparée synthétisée dans l'étude préalable au Livre vert de la Comission européenne précité : Hydra Associates, The Protection of Minors and human Dignity in the Information Society - Analysis and Options, Londres, 1996. Voir aussi l'annexe III du Livre vert de la Commission précité

Une autre voie, toujours sur le plan réglementaire international, est le renforcement de la coopération judiciaire et policière. On citera à cet égard tant la Communication de la Commission ainsi que son Livre vert sur la protection des mineurs et de la dignité humaine dans les nouveaux services audiovisuel et d'information, tous deux précités, qui prônent le renforcement de cette coopération, ne fût-ce que dans l'échange d'informations, de manière préventive.

A cet égard, le Traité sur l'Union européennc consacre en son Titre IV le rôle de l'Union sur le plan de la coopération en matière de justice et d'affaires intérieures. Ce nouvel instrument nous paraît particulièrement adapté pour une approche à tous le moins concertée de la criminalité transnationale véhiculée par Internet.

V.2. L'autoréglementation

Il semble qu'à côté des solutions de coopération internationale intergouvernementale, qui ne peuvent viser que le moyen ou le long terme, l'élaboration de codes de conduite présente une solution complémentaire non négligeable dans le contexte d'Internet. Ces instruments présentent en effet souvent l'avantage de pouvoir s'adapter rapidement à l'évolution technique, puisqu'ils sont l'oeuvre des acteurs des marchés concernés.

On renverra avec intérêt, sur ce point, à l'exemple du code de conduite proposé par la Safety Net Foundation au Royaume-Uni[434].

Ce projet de code, qui est une initiative industrielle[435], se fonde sur trois principes de base :

1. La classification des contenus préjudiciables, par la Safety Net Foundation (SNF). On notera cependant que de telles classifications ne sont pas aisées dans l'environnement mouvant, voire volatile, d'Internet. La SNF entend promouvoir dans cette optique le standard de filtrage relativement souple Platform for Internet Control Selection (PICS)[436];
2. La mise à disposition d'un système de points-contacts[437] (que l'on pourrait comparer à des numéros verts électroniques) permettant aux utilisateurs des services de se plaindre du contenu de certains services;

434 Voir notamment sur ces propositions : « R3 Safety Net · Rating, Reporting, Responsibility For Child Pornography and Illegal Material on the Internet », London, 1996.

435 Ces propositions ont été exprimées notamment par des fournisseurs d'accès ainsi que par les plus importants fournisseurs de services du royaume-Uni.

436 Voir ci-dessous.

437 « Hot line services ».

3. La conséeration d'un principe de responsabilité des fournisseurs de services qui, ayant été informés de la présence de contenus illégaux ou préjudiciables, ne retireraient pas des pages identifiées ou ne prendrait pas les mesures qui s'imposent. Dans ce cas, les faits seraient dénoncés aux services de police britanniques compétents.

Cette voie doit être analysée en parallèle avec les systèmes de points-contacts en plein développement actuellement, dans un premier temps indépendamment de toute initiative autorégulatrice des acteurs concernés. On mentionnera ainsi l'existence, en Belgique, de plusieurs initiatives principales de ce type en matière de pornographie enfantine[438], qui s'inspirent d'ailleurs d'un système néerlandais.

Il reste que l'élaboration de codes de conduite pose le problème de la représentativité des divers acteurs concernés. Si les industriels sont souvent présents dans les associations qui élaborent ces textes, il n'en est pas toujours de même des utilisateurs eux-mêmes, concernés au premier chef par les pratiques que ces codes entendent réguler. A cet égard, on peut renvoyer à l'intéressante initiative australienne Initia, qui propose un « Internet Industry Code of Practice »[439]. Outre son caractère relativement élaboré, on mentionnera la volonté de voir gérer ce code par un « Administrative Council » comprenant notamment un représentant du ministère fédéral des télécommunications, des représentants de l'industrie, mais également un représentant des utilisateurs. Ce projet de code privilé-

438 Par exemple, le Meldpunt Kinderpornografie (kinderporno@meldpunt.be), le Belgisch Burgerlijk Digitaal Meldpunt » (ping ne/ping7367/meldpunt.html) ou, plus récemment, le site de la police judiciaire elle-même. Ce dernier site, intitulé « Point de contact pornographie enfantine » a été élaboré par la cellule nationale « Pornographie sur Internet » de la police judiciaire. On lira avec intérêt le texte présenté sur ce site (CONTACT@gpj.be) :

« La diffusion de matériel pornographique est punie comme outrage public aux bonnes moeurs par l'article 383 du Code pénal La peine est plus sévère quand l'outrage public aux bonnes moeurs est commis en présence de mineurs d'âge, vu les articles 386 et 386 bis du code pénal »

« Ces dispositions de loi pénalisent toute forme d'outrage public aux bonnes moeurs, que ce soit par le biais de publications imprimées, d'images ou de figures ou par des moyens audiovisuels »

« Celui qui, via un réseau informatique, expose ou diffuse du matériel pornographique, sera donc punissable sans que l'intention de profit ne soit démontrée »

« En outre, un article 383bis, qui pénalise la pornographie enfantine, a été inséré dans la loi du 13 avril 1995 »

« Suivant cet article, n'est pas seulement punissable celui qui aura exposé, vendu, loué, distribué, remis, fabriqué, etc. de la pornographie enfantine, mais également celui qui en aura détenu »

« La distribution de pornographie enfantine, via un réseau informatique, comme le dépôt dans un autre forum d'images ou écrits pornographiques impliquant des mineurs, peut donc être punie sur base de la législation actuelle. De même, la possession de tels écrits ou images sur disque dur ou sur tout support électronique ou optique, tombe sous le coup des dispositions de cette loi, au sens large (par exemple, le téléchargement sur disque dur de pornographie enfantine). »

« Si, en tant que citoyen, vous êtes confronté sur Internet à un cas de pornographie tel que images à caractère pédophilique, prière d'en avertir la cellule nationale « Pornographie enfantine sur Internet », qui a été créée dans ce but au sein de la Police Judiciaire »

A partir d'aujourd'hui, vous pouvez aussi avertir la cellule via Internet La Police Judiciaire a, dans ce but, officiellement installé un point de contact national à l'adresse E-mail spécifique suivante CONTACT@gpj.be, prière de communiquer le plus complètement possible les coordonnées de ce que vous avez constaté par exemple, l'url du site web ou la provenance exacte du nouveau message ». L'utilisation d'un formulaire électronique est également prévue par la police judiciaire

439 L'adresse Internet de ce code est ( )conduct@initiaa.asn au

gie également les systèmes correspondant au standard de filtrage PICS susmentionné.

Comme on peut le constater, la promotion de codes de conduite va de pair avec la volonté affichée de voir se développer des systèmes techniques de filtrage.

V.3. Les solutions techniques

Si la technologie permet le développement de nouvelles formes de criminalité, elle permet également l'élaboration de systèmes techniques favorisant la prévention de ces infractions. L'industrie électronique a notamment mis sur le marché des logiciels de filtrage. Ces systèmes techniques de filtrage fonctionnent généralement selon l'un des trois principes suivants[440] :

1. Un système de « liste noire » de sites ou d'adresses constituées auxquels l'utilisateur ne peut accéder étant donné le blocage réalisé par un logiciel, étant donné le type d'information qui s'y retrouve[441];
2. Un système de liste blanche, mettant en oeuvre le principe inverse, à savoir l'autorisation d'accès aux seuls sites ou adresses présélectionnées dans le logiciel. Ce système particulièrement restrictif est par exemple utilisé par des établissements scolaires.
3. Un système de « labellisation » ou de classification neutre de contenus. Dans ce système, relativement récent, les sites ou adresses se voient attribuer un label neutre de valeur qui est paramétré (« coté ») ensuite par l'utilisateur ou par un tiers (le fournisseur de services, une association quelconque, etc.). La norme Platform for Internet Content Selection (PICS), permettant d'éviter la censure générale en séparant fonctionnellement l'échelle de classification et la classification elle-même (le « rating »), est particulièrement prônée par l'industrie et concilie sans doute en effet de manière souple la liberté d'expression et les restrictions légitimes qu'un particulier veut imposer aux utilisateurs (notamment les mineurs, les employés d'une entreprise) de son ou ses ordinateur(s).

Quel que soit cependant le degré de développement de ces systèmes de filtrage, il apparaît que ceux-ci correspondent plutôt à l'aspiration (légitime) de certains de restreindre l'accès à certains contenus et ne permettent pas de réprimer des contenus illégaux en soi. Comme le reconnaît

440 Voir, sur ce point, la Communication de la Commission européenne précitée, p. 18 et suivantes. Voir également les développements consacrés à ce sujet dans la « preliminary injunction » ACLU vs RENO précitée.

441 Par exemple dans le cas du logiciel Cyberpatrol : violence, nudité, actes sexuels, drogue, cultes sataniques, extrémisme, jeux, alcool, tabac, etc.

la Commission elle-même, ces solutions sont d'ailleurs plus pragmatiques que, à proprement parler, légales.

En conclusion de cette brève analyse, on constatera d'une part que les diverses solutions esquissées ci-dessus apparaissent complémentaires plutôt qu'exclusives l'une de l'autre. Cette complémentarité peut seule permettre le développement harmonieux de la communication électronique sur Internet.

D'autre part, ces solutions complémentaires mettent en lumière, en définitive, la nécessité de la contribution, chacun à leur niveau de responsabilité, des différents acteurs concernés par la communication sur Internet : les Etats et les institutions internationales, les opérateurs du marché et, finalement, les utilisateurs de ces services.